Den Haag

# Aansluitvoorwaarden SFTP-GW

Versie 1.5

Status <Definitief>

02 juni 2018

Auteur: Alex Schreuder, Dave Brinkert, Ferry Schuller, David Markus, Rene Hoogvliet, Peter van Eijk

## Colofon

| | |
|---|---|
| Titel | **Aansluitvoorwaarden SFTP-GW** |
| Ondertitel | Aansluitvoorwaarden SFTP-GW |
| Versie, datum | 1.5 , 6-juli 2018 |
| Referentie | |
| Samengesteld door | Alex Schreuder, Dave Brinkert, Ferry Schuller, David Markus, Rene Hoogvliet, Peter van Eijk |
| Bestandsnaam | https://samenwerken.denhaag.nl/teams/t17_0207/DS01/Proces3/SFTP-Gateway/Aansluitvoorwaarden SFTP-GW v1.5.docx |

# Inhoudsopgave

# 1. Inleiding

## 1.1. Doel van dit document

Informeren van de afnemers van deze service over de vereisten waaraan moet worden voldaan om gebruik te kunnen maken van deze dienstverlening. Onder afnemers verstaan we functioneel beheerders en externe partijen die zaken doen met de gemeente.

## 1.2. Referenties

De uitwisseling van gegevens op een betrouwbare wijze is van groot belang. In dat kader speelt de Baseline Informatiebeveiliging Gemeente (BIG) en de toepassing daarvan een belangrijke trol.

| # | Referentie | Document |
|---|---|---|
| 1 | BIG | Baseline Informatiebeveiliging Gemeente |
| 2 | | Beleidskader Informatieveiligheid 2015-2018 |
| 3 | | Regeling bestandsuitwisseling (concept) |

## 1.3. Afkortingen en begrippen

Aangezien dit document voor diverse doelgroepen bedoeld is, is het in algemene zin belangrijk dat de voornaamste begrippen en afkortingen op een eenduidige manier geïnterpreteerd worden. Hieronder zijn deze nader verklaard.

| Afkorting | Toelichting |
|---|---|
| ISO | Information Security Officer |
| FTP | File Transfer Protocol.  Netwerkprotocol voor bestandsoverdrachten. Hierbij kunnen alleen geautoriseerde klanten een verbinding opzetten, maar er wordt geen gebruik gemaakt van encryptie. FTP verkeer zonder encryptie is niet toegestaan volgens onze normering. |
| NSW | Niet-Standaard Wijziging |
| sTFP | Secure File Transfer Protocol. Een op FTP-gebaseerd netwerkprotocol voor bestandsoverdrachten die verlopen via SSH. Hierbij wordt gebruik gemaakt van encryptie tijdens authenticatie en dataverkeer.  Omdat de gegevens en inlogwachtwoorden door middel van deze methode bij onderschepping op het internet versleuteld zijn is deze manier van bestandsuitwisseling voldoende veilig en geaccepteerd. |

# 2. Beschrijving product/dienst

De sFTP-Gateway levert een service voor het uitwisselen van bestanden waarbij gebruik wordt gemaakt van een veilig protocol. Vanuit functionele scheiding en verhogen van continuïteit van de service wordt de service aangeboden uit zowel een interne als externe variant. Waarbij de externe service wordt ingezet voor bestandsoverdracht tussen de gemeente en een externe partij. De interne service wordt beschikbaar gesteld voor de bestandsoverdracht tussen interne systemen. Voor deze diensten gelden de volgende *principes*:

- De sFTP-Gateway extern initieert de bestands-transfer, tenzij;
- "Store & forward" datatransfer, retentie tijden zijn daarbij gekoppeld aan dataclasificatie (zie tabel 2.1.1);
- Toepassing van Secure FTP protocol;
- De file transfer past binnen de logische capaciteiten van het netwerk en de systemen.

Kenmerkend is dat tijdens authenticatie en de uitwisseling van data gebruik gemaakt wordt van encryptie. Zowel de gemeente als de externe partij identificeert zich middels certificaten. Over het transport vindt logging plaats bij deze dienstverlening zodat kan worden aangetoond wanneer het transport heeft plaatsgevonden, middels welk account en of dit foutloos is geweest of niet. Deze logging wordt standaard 6 maanden bewaard.
Om de integriteit en vertrouwelijkheid van data beter te kunnen garanderen wordt er gebruik gemaakt van een geïsoleerde container. Binnen deze container(s) zijn de retentietijden inzake dataclassificatie van toepassing.

## 2.1. Afbakening & beperkingen

Voor gegevens uitwisseling tussen partijen geldt het architectuur principe "de WS-Gateway, tenzij". De sFTP-Gateway is dus een alternatief, speciaal bedoeld voor het uitwisselen van bestanden. Echter met als beperking dat deze dienst niet geschikt wordt geacht voor overdracht van "Strikt Vertrouwelijk" geclassificeerde bestanden.
**Deze service is bedoeld voor periodieke bestandsuitwisseling (met externe partijen), waarbij uitwisseling van bestanden via webservices niet mogelijk of haalbaar is.**
Voor data met classificatie vertrouwelijk dienen additionele maatregelen te worden genomen om de data te beschermen. De data zelf dient te zijn versleuteld, voorzien van een wachtwoord en dit wachtwoord dient via een ander medium gedeeld te worden met de ontvangende partij.

### 2.1.1. Retentie tijden

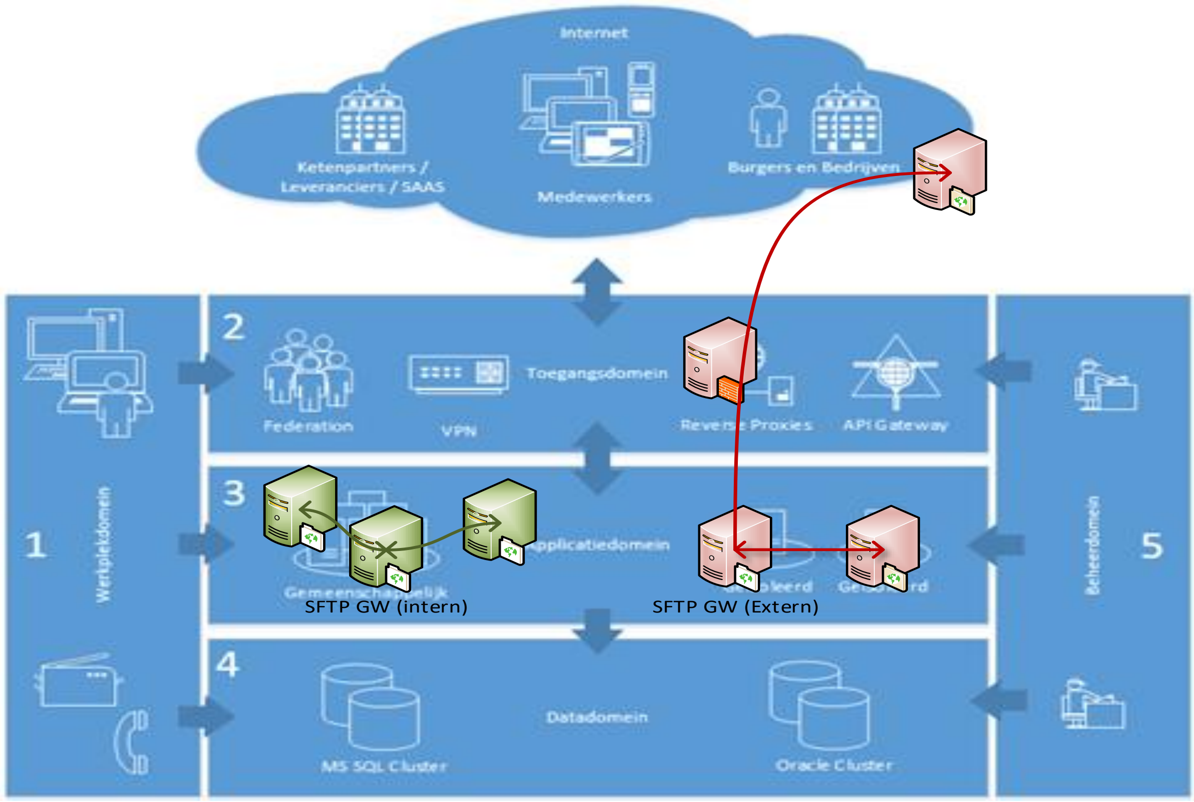
| Data Classificatie | Retentie tijd[1] | Extra maatregel |
|---|---|---|
| Openbaar | 12 uur | |
| Intern | 8 uur | |
| Vertrouwelijk | 4 uur | *Versleuteling van het bestand is hierbij van kracht* |
| Strikt Vertrouwelijk | Let op: data uitwisseling o.b.v. sFTP is voor deze data klasse niet toegestaan.<br>NB: Uitzonderingen worden via de ISO o.b.v. 'pas-toe-of-leg-uit' nader geanalyseerd. | |

[1] Vanuit beheer zal logging aantonen of aan deze verplichtingen wordt voldaan

## 2.2. Functionaliteit

Veilige bestand overdracht service voor periodieke en herhaaldelijke bestandsoverdracht doeleinden.

## 2.3. Architectuur



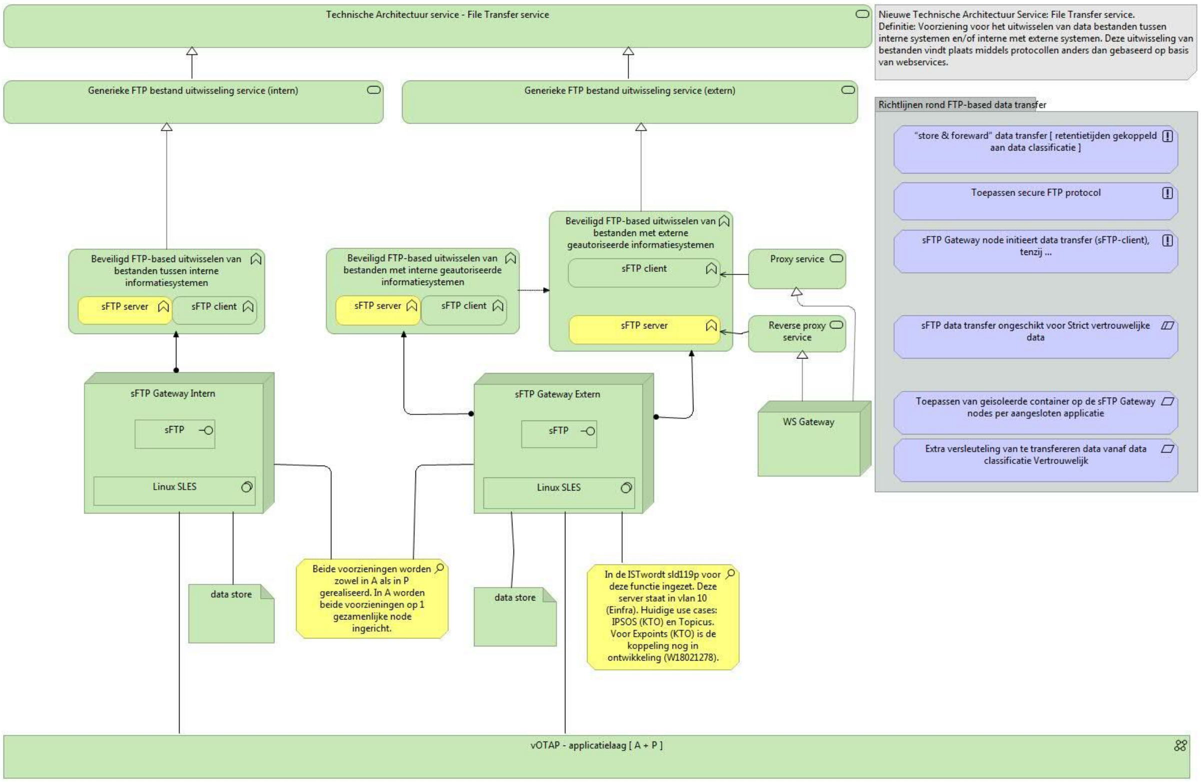

Figuur 2-1 De generieke sFTP voorziening in vOTAP.

Bovenstaande Figuur 2-1 geeft vereenvoudigd de architectuur weer. Deze weergave geeft een overzicht van functioneel domeinen met security boundaries conform vOTAP. Dit is tevens de weergave van de SOLL-situatie. Vanuit klantbehoefte wordt de service ook aangeboden vanuit de bestaande E-infra omgeving (sftp-gateway.prod.haagnet.net).

De realisatie in de E-infra wijkt enigszins af[2]. De reden daarvan is dat er al enkele sFTP stromen zijn gerealiseerd in de E-infra voordat de generieke sFTP dienst is uitgewerkt. De E-infra wordt vanaf 2018 gefaseerd via een ‘sterfhuisconstructie’ afgebouwd. De vOTAP is de vervangende omgeving waarin de generieke dienst als afgebeeld wordt opgebouwd. Derhalve is gekozen voor een enigszins afwijkende implementatie om de bestaande sFTP-toepassingen in de E-infra zo min mogelijk te verstoren.

Onderstaande archimate plaat (verduidelijkt een aantal specifieke details in relatie tot de sFTP-GW services.

[2] Zie bijlage 1 voor de afwijkingen van de implementatie van de generieke sFTP voorziening in de E-infra.




Figuur 2-2 Archimate View van de sFTP voorziening in de Technische Architectuur.

De verkeersstromen van binnen naar buiten en vice versa verlopen standaard via een proxy voorziening in het toegangsdomein. Dit wordt in de paragrafen 2.4.1 en 2.4.2 nader toegelicht.
Voor het ontvangen en versturen van de betreffende bestanden (volgens het store and forward principe) wordt gebruik gemaakt van storage op de sFTP-GW. De requirement daarbij is dat **per applicatie een geïsoleerde container** op de sFTP-Gateway wordt toegepast. Verder gelden de retentie tijden zoals eerder aangegeven in paragraaf 2.1.1.
De storage is gecompartimenteerd en toegankelijk volgens RBAC. Als aanvullende requirement geldt dat als *Vertrouwelijk* geclassificeerde bestanden door de data-eigenaar[3] versleuteld dienen te worden voor transport. De verantwoordelijkheid van de versleuteling ligt bij de data-eigenaar.

De <u>sFTP-GW Intern</u> voorziening bestaat in de Ontwikkel/Test(OT), Acceptatie (A) en Productie (P) omgevingen van vOTAP en E-infra. De <u>sFTP-GW Extern</u> voorziening bestaat alleen in de Acceptatie (A) en Productie (P) omgevingen van vOTAP en E-infra. Op termijn zullen deze voorzieningen worden gemigreerd naar het Central services domein.

NB: binnen het Beheerdomein van vOTAP wordt een aparte *Beheer sFTP-GW* voorziening ingericht. Deze voorziening maakt <u>geen</u> onderdeel uit van de generieke bestanduitwisseling service welke in dit document wordt beschreven. De *Beheer SFTP-GW* voorziening dient alleen, zoals de naam al aangeeft, data transfer t.b.v. het technisch beheer van de ICT-infrastructuur van de gemeente.

[3] Dit kan ook een gedelegeerde functionaris zijn. Een functioneel beheerder kan bijvoorbeeld als gedelegeerde van de data-eigenaar acteren in dit proces.

## 2.4. Scenario's en aansluitvoorwaarden

### 2.4.1. Bestandsoverdracht van/naar een externe partij

Daarbij zijn de volgende scenario's van toepassing:

1. Een externe partij biedt periodiek een bestand aan voor de gemeente;
2. De gemeente biedt periodiek een bestand aan voor een externe partij.

**Bij voorkeur initieert de SFTP-Gateway Extern in beide gevallen de overdracht van het bestand.** De sFTP-Gateway Extern fungeert als sFTP-client en verloopt de verkeersstroom via de proxy service voorziening ('cache proxy').
In voorkomende gevallen waar het echt niet anders mogelijk is, kan de sFTP-Gateway Extern de functie van sFTP-server vervullen. De sFTP verkeersstroom loopt in dat geval per definitie via de WS-Gateway (extern), die hierin dan de reverse proxy functie vervult door virtueel een sFTP server service aan te bieden aan de buitenkant. In dit geval zijn ook de aansluitvoorwaarden van de WS-Gateway van kracht. Tevens bied deze solution extra functionaliteit omdat deze virtueel aangeboden sFTP server service via HTTP benaderd kan worden aan de buiten zijde.

| Scenario | Rol Externe Partij | Rol SFTP-Gateway | Proxy | Interne bron/doel |
|---|---|---|---|---|
| Externe partij biedt bestand aan | sFTP Server | sFTP Client (Initieert) | Cache | sFTP Client of server |
| Externe partij biedt bestand aan | sFTP Client (Initieert) | sFTP Server | WS-GW | sFTP Client of server |
| Gemeente DH biedt bestand aan | sFTP Server | sFTP Client (Initieert) | Cache | sFTP Client of server |
| Gemeente DH biedt bestand aan | sFTP Client (Initieert) | sFTP Server | WS-GW | sFTP Client of server |

#### 2.4.1.1 Aansluitvoorwaarden interne component

De interne (bron|afnemende) server mag data bestanden direct o.b.v. sFTP aanleveren op, of afnemen van, de SFTP-Gateway Extern. Het aanvragen van een FW-ontheffing is echter een voorwaarde om dit verkeer mogelijk te maken.

### 2.4.2. Interne bestandsoverdracht

Analoog aan het principe voor externe bestandsuitwisseling zal bestandoverdracht tussen interne servers via de sFTP-Gateway Intern verlopen. Echter, voor interne bestandsuitwisselingen is het **niet** nodig om de verkeersstromen via de cache proxy of WS-Gateway voorziening te laten verlopen. Ook is er geen specifieke voorkeur of vereiste aangaande de client en server rol bij interne transfers. Dit wordt mede bepaald door het gebruikte platform, Windows servers zijn standaard niet voorzien van de SFTP server rol. Daarin tegen Unix/Linux servers wel.

# 3. Aanvragen product/dienst bestandsuitwisseling met Externe partij

Vanuit het Changemanagement van de gemeentelijke Dienst wordt een NSW ingediend bij IDC/A, een NSW “Periodieke bestandsuitwisseling met externe partij via sFTP”. Voorafgaande aan de aanvraag heeft de dataclasificatie plaatsgevonden en is deze behoefte intern met de ISO afgestemd zodat er geen onduidelijkheid is of een dergelijke uitwisseling van bestanden/gegevens is toegestaan. De verantwoordelijkheid hiervoor ligt bij de aanvrager.

## 3.1. Verplichtingen afnemer

De afnemende en opdracht gevende partij draagt verantwoording om conform Privacywetgeving te handelen indien er sprake is van privacy gevoelige gegevens die uitgewisseld gaan worden. Dit kan betekenen dat er een PIA (Privacy Impact Analyse) vooraf dient te worden uitgevoerd. Verder dient er conform de BIG, dataclassificatie normeringsmaatregelen te worden gehandeld. Dit kan bijvoorbeeld betekenen dat vertrouwelijke bestanden versleuteld dienen te zijn voordat er transport plaatsvindt en een geheimhoudingsverklaring is getekend. De aanvrager en gebruiker van de dienst is daarvoor verantwoordelijk en dient zelf voor afstemming met de ISO te zorgen zodat er duidelijkheid is over de te treffen maatregelen. Het IDC, de uitvoerende partij, verzorgt alleen de technische bestandsoverdracht volgens geldende normering en beleid.

## 3.2. Werkzaamheden/voorbereiding

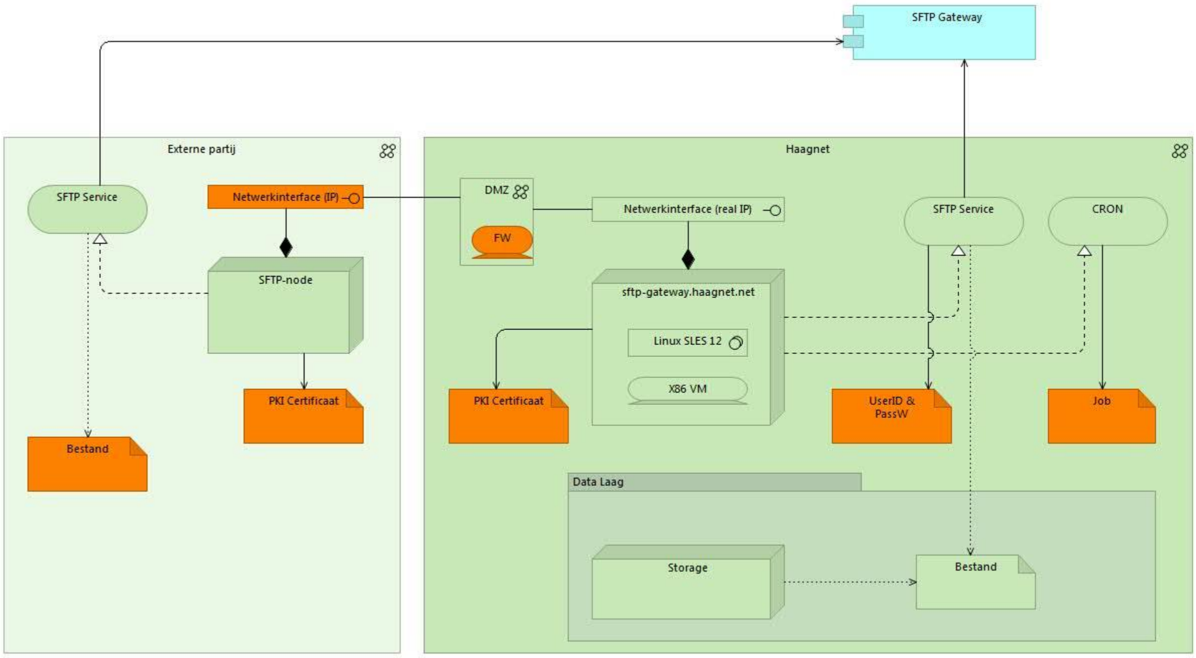
Vanuit de gemeentelijke Dienst wordt er een NSW ingediend bij IDC/A, voorzien van de benodigde informatie (zie 3.2.1).

### 3.2.1. Aan te leveren gegevens

De volgende informatie is benodigd voor het doen van de aanvraag en dienen te worden aangeleverd vanuit de dienst (aanvrager):

1. De aanvrager heeft intern afgestemd dat de ISO akkoord is met de inhoudelijke gegevensuitwisseling, of wel dat de ontvangende partij deze gegevens mag ontvangen/inzien en noodzakelijke verplichtingen daartoe zijn getroffen (zie 3.1).
2. IP adres host externe partij (waar bestand dient te worden geplaats / opgehaald).
3. PKI-certificaat externe partij.
4. Bestand(snaam) voor overdracht.
5. Plaats & locatie van het te plaatsen / op te halen bestand
   a. Bron locatie
   b. Doel locatie
6. Toegang: UserID & password (of Private Key) – gescheiden aanleveren.
7. Tijdstip en frequentie van het op te halen / plaatsen bestand.
8. Te informeren personen (e-mail adressen) bij geslaagde en niet geslaagde bestandsoverdracht.
9. Verzendende partij: Naam van de partij en contactpersoon gegevens, zoals naam, e-mail adres en telefoonnummer.
10. Ontvangende partij: Naam van de partij en contactpersoon gegevens, zoals naam, e-mail adres en telefoonnummer.
11. Bij uitwisseling met externe, een extern technisch contact persoon voor beheer doeleinden.

Onderstaande architectuur plaat Figuur 3-1 geeft in oranje weer welke objectgegevens van belang zijn om de bestandsuitwisseling technisch te kunnen opzetten.




Figuur 3-1 Archimate View met de in scope zijnde infrastructuur componenten voor een data uitwisseling o.b.v. sFTP.

Uit te voeren activiteiten (op hoofdlijnen) voor de realisatie van een op sFTP gebaseerde bestandsuitwisseling:

1. Het IP adres van de cache.haagnet.net wordt op de FW van de externe partij opgevoerd om sFTP verkeer over poort 22 mogelijk te maken. Echter, indien het verkeer geïnitieerd dient te worden vanuit de externe partij gelden de aansluitvoorwaarden van de WS-Gateway. Het IP adres van de host (van de externe partij) is daarbij noodzakelijk om te worden opgevoerd in de FW van Den Haag.
2. PKI-certificaten worden uitgewisseld en geïnstalleerd, zodat de identiteit van de host met voldoende zekerheid kan worden vastgesteld en authenticatie en verkeer versleuteld kunnen worden.
3. Er worden (cron) jobs gecreëerd voor bestandsoverdracht tussen de sFTP-Gateway en de externe partij) tussen sFTP-Gateway (extern) en externe host, en voor de overdracht tussen de sFTP-Gateway en de interne (leverende | doel) server. Randvoorwaarden: de toegang tot host en bestand wordt via UserID en password gereguleerd. E-mail adressen zijn noodzakelijk om de gebruiker geautomatiseerd te kunnen informeren over de status van de gedane bestandsoverdracht.
4. Per toepassing (lees: sFTP data uitwisseling tussen twee interne servers of een interne en externe server) wordt er een geïsoleerde omgeving (container) gevormd waarvan de storage toegankelijk wordt gemaakt volgens RBAC.
5. Het koppelen van de interne component, zoals aangegeven in paragraaf 2.4.1.1.

**NB1**: in het uitzonderlijke geval de SFTP-GW Extern bij de data uitwisseling met een externe partij de rol van sFTP-server heeft, dient er tevens een configuratie aanpassing op de WSG-Extern plaats te vinden. Het IP adres van de externe sFTP host dient opgevoerd te worden in de WSG-Extern.
**NB2**: bovenstaande activiteit 1 is uiteraard niet nodig indien het data uitwisseling betreft tussen 2 interne servers via de sFTP-GW Intern. Volgend hoofdstuk is hier specifiek over.

# 4. Aanvragen product/dienst bestandsuitwisseling met interne partij

Dit hoofdstuk dient om duidelijkheid te verschaffen in de interne aansluitvariant voor de lezer, voor enkel bestandsoverdracht tussen interne partijen/server. Ook al komt dit hoofdstuk voornamelijk overeen met het voorgaande, er zijn enkele nuance verschillen. Middels een NSW "Periodieke interne bestandsuitwisseling via sFTP" vanuit het Changemanagement van de gemeentelijke Dienst wordt een NSW ingediend bij IDC/A.
Voorafgaande aan de aanvraag heeft de dataclasificatie plaatsgevonden en is deze behoefte intern met de ISO afgestemd zodat er geen onduidelijkheid is of een dergelijke uitwisseling van bestanden/gegevens is toegestaan. De verantwoordelijkheid hiervoor ligt bij de aanvrager.

## 4.1. Verplichtingen afnemer

De afnemende en opdracht gevende partij draagt verantwoording om conform Privacywetgeving te handelen indien er sprake is van privacy gevoelige gegevens die uitgewisseld gaan worden. Dit kan betekenen dat er een PIA (Privacy Impact Analyse) vooraf dient te worden uitgevoerd. Verder dient er conform de BIG, dataclassificatie normeringsmaatregelen te worden gehandeld. Dit kan bijvoorbeeld betekenen dat vertrouwelijke bestanden versleuteld dienen te zijn voordat er transport plaatsvindt en een geheimhoudingsverklaring is getekend. De aanvrager en gebruiker van de dienst is daarvoor verantwoordelijk en dient zelf voor afstemming met de ISO te zorgen zodat er duidelijkheid is over de te treffen maatregelen. Het IDC, de uitvoerende partij, verzorgt alleen de technische bestandsoverdracht volgens geldende normering en beleid.

## 4.2. Werkzaamheden/voorbereiding

Vanuit de gemeentelijke Dienst wordt er een NSW ingediend bij IDC/A, voorzien van de benodigde informatie (zie 4.2.1).

### 4.2.1. Aan te leveren gegevens

De volgende informatie is benodigd voor het doen van de aanvraag en dienen te worden aangeleverd vanuit de dienst (aanvrager):

1. De aanvrager heeft intern afgestemd dat de ISO akkoord is met de inhoudelijke gegevensuitwisseling, of wel dat de ontvangende partij deze gegevens mag ontvangen/inzien en noodzakelijke verplichtingen daartoe zijn getroffen (zie 4.1).
2. Servernaam/IP adres waar bestand dient te worden geplaats / opgehaald.
3. Bestand(snaam) voor overdracht.
4. Plaats & locatie van het te plaatsen / op te halen bestand
    a. Bron locatie
    b. Doel locatie
5. Toegang: UserID & password (of Private Key) – gescheiden aanleveren.
6. Tijdstip en frequentie van het op te halen / plaatsen bestand.
7. Te informeren personen (e-mail adressen) bij geslaagde en niet geslaagde bestandsoverdracht.
8. Verzendende partij: Naam van de partij en contactpersoon gegevens, zoals naam, e-mail adres en telefoonnummer.
9. Ontvangende partij: Naam van de partij en contactpersoon gegevens, zoals naam, e-mail adres en telefoonnummer.

Uit te voeren activiteiten (op hoofdlijnen) voor de realisatie van een op sFTP gebaseerde interne bestandsuitwisseling:

1. Er worden (cron) jobs gecreëerd voor bestandsoverdracht tussen de sFTP-Gateway intern voor de overdracht tussen de sFTP-Gateway en de interne servers (leverende en doel server).
   Randvoorwaarden: de toegang tot host en bestand wordt via UserID en password gereguleerd. E-mail adressen zijn noodzakelijk om de gebruiker geautomatiseerd te kunnen informeren over de status van de gedane bestandsoverdracht.
2. Per toepassing (lees: sFTP data uitwisseling tussen twee interne servers) wordt er een geïsoleerde omgeving (container) gevormd waarvan de storage toegankelijk wordt gemaakt volgens RBAC.

# 5. Ondersteuning, exploitatielasten en onderhoud

Tenzij anders geregeld (per aanvraag) is de standaard DVO van toepassing.
Ondersteuning zal via de reguliere helpdesk en beheerafdeling worden verleend na het melden van een incident of NSW.
Het standaard onderhoud valt onder de getekende algemene DVO.

# Bijlage 1: Toelichting sFTP Gateway voorziening E-infra

In paragraaf 2.3 wordt gemeld dat de implementatie van de generieke sFTP voorziening in de E-infra omgeving enigszins afwijkt van de wijze in vOTAP.

De reden daarvan is dat er al enkele sFTP stromen zijn gerealiseerd in de E-infra voordat de generieke sFTP dienst is ontworpen en ontwikkeld.
De E-infra wordt vanaf 2018 gefaseerd via een ‘sterfhuisconstructie’ afgebouwd. De vOTAP is de vervangende omgeving, waarin de generieke sFTP bestanduitwisseling service wordt opgebouwd. Derhalve is gekozen voor een enigszins afwijkende implementatie om de bestaande sFTP-toepassingen in de E-infra zo min mogelijk te verstoren.

De afwijkingen zijn:

- De sFTP-GW voorziening is in de E-infra gehost in de Datalaag. Dit betekent dat de sFTP-GW Intern gepositioneerd is in vlan 60 (A: vlan 660) en de SFTP-GW Extern in vlan 10 (A: vlan 670).
- Bij bestanduitwisseling via de sFTP-GW Extern verloopt de verkeersstroom niet via de WSG-Extern. Dit verkeer verloopt direct via de E-infra firewall waar IP-source NAT plaatsvindt naar een publiek IP-adres van de gemeente.

Voor de realisatie van op sFTP gebaseerde data uitwisselingen in de E-infra geldt dat deze te allen tijde ontheffing plichtig is. De bijbehorende FW-aanvragen zullen doorgaans worden gehonoreerd. Deze procedure dient ter auditing doeleinden vanuit security.

# Bijlage 2: Overzicht SFTP Solutions

Onderstaand overzicht geeft inzage in de sFTP toepassingen per april 2018.